Int. J. Math. And Appl., 7(1)(2019), 137–148
ISSN: 2347-1557
Available Online: http://ijmaa.in/

International Journal of Mathematics And its Applications

Implementing Wiener's Extensions in the Range $N^{\frac{1}{4}} \leq d < N^{\frac{3}{4}-\beta}$ and $N^{\frac{1}{4}} \leq d < N^{(\frac{1-\gamma}{2})}$, $\gamma \leq \frac{1}{2}$ with Lattice Reduction

P. Anuradha Kameswari[1,*] and S. B. T. Sundari Katakam[1]

1 Department of Mathematics, Andhra University, Visakhapatnam, Andhra Pradesh, India.

Abstract: In this paper, Wiener Attack extensions on RSA are implemented with approximation via lattice reduction. The continued fraction based arguments of Wiener Attack extensions in the range $N^{\frac{1}{4}} \leq d < N^{\frac{3}{4}-\beta}$, $p-q = N^{\beta}$ and $N^{\frac{1}{4}} \leq d < N^{(\frac{1-\gamma}{2})}$, $|\rho q - p| \leq \frac{N^{\gamma}}{16}$, $1 \leq \rho \leq 2$, $\gamma \leq \frac{1}{2}$, are implemented with the Lattice based arguments and the LLL algorithm is used for reducing a basis of a lattice.

MSC: 11T71, 94A60.

Keywords: Lattice reduction, LLL algorithm, quadratic form, Wiener Attack extensions.

1. Introduction

Wiener's attack on RSA applies when the private exponent d is less than $N^{\frac{1}{4}}$. Whenever $d < \frac{N^{1/4}}{\sqrt{6}}$, the fraction $\frac{t}{d}$ is a convergent of $\frac{e}{N}$ and hence it is an approximation of $\frac{e}{N}$ and thus (d,t) may be obtained as a short vector by reducing the quadratic form $q(x,y) = M\left(\frac{e}{N}x - y\right)^2 + \frac{1}{M}x^2$ for an appropriate choice of M [8]. Now we adapt these ideas to Wiener Attack extensions in the range $N^{\frac{1}{4}} \leq d < N^{\frac{3}{4}-\beta}$, $p-q = N^{\beta}$ and $N^{\frac{1}{4}} \leq d < N^{(\frac{1-\gamma}{2})}$, $\gamma \leq \frac{1}{2}$ with lattice reduction.

2. Implementing Wiener's Extension in the Range $N^{\frac{1}{4}} \leq d < N^{\frac{3}{4}-\beta}$ with Lattice Reduction

This section shows that for the bound of private exponent d in RSA, extended to N^{δ}, where $\frac{1}{4} \leq \delta < \frac{3}{4}-\beta$ and $\Delta = p-q = N^{\beta}$, $\beta \in (\frac{1}{4}, \frac{1}{2})$, the attack may be implemented with lattice reduction. We first recall an estimation for $\varphi(N)$ and show that with this estimation we may consider a quadratic form and using this quadratic form, (d,t) may be obtained as a short vector of the quadratic form for some appropriate M.

Lemma 2.1. *Let $N = pq$ where p,q are primes such that $q < p < 2q$ and $\Delta = p - q$. Then* $0 < p + q - 2N^{\frac{1}{2}} < \frac{\Delta^2}{4N^{\frac{1}{2}}}$.

Lemma 2.2. *An estimation of $\varphi(N)$ when $q < p < 2q$ is given by*

$$N + 1 - \frac{3}{\sqrt{2}}N^{\frac{1}{2}} < \varphi(N) < N + 1 - 2N^{\frac{1}{2}}.$$

* *E-mail: panuradhakameswari@yahoo.in*

This estimation plays an important role in the following theorem.

Theorem 2.3. Let $p - q = \Delta = N^{\beta}$ and $d = N^{\delta}$, where $q < p < 2q$, $d < N^{\frac{3}{4}-\beta}$. Then

$$\left|\frac{e}{N+1-2N^{\frac{1}{2}}} - \frac{t}{d}\right| < \frac{1}{2d^2}.$$

Hence by approximation theorem it follows that $\frac{t}{d}$ is a convergent of $\frac{e}{N+1-2N^{\frac{1}{2}}}$. Thus, $\frac{t}{d}$ is obtained from the list of convergent of $\frac{e}{N+1-2N^{\frac{1}{2}}}$ using continued fractions. Wiener's extension attack on RSA basically searches the convergent $\frac{t}{d}$ from the class of convergent of $\frac{e}{N+1-2N^{\frac{1}{2}}}$ that lead to (p, q, d) whenever $N^{\frac{1}{4}} \leq d < N^{\frac{3}{4}-\beta}$, $p - q = N^{\beta}$.

Theorem 2.4 (Wiener's extension in the range $N^{\frac{1}{4}} \leq d < N^{\frac{3}{4}-\beta}$)**.** *Let $N^{\frac{1}{4}} \leq d < N^{\frac{3}{4}-\beta}$, $p - q = N^{\beta}$ and for any convergent $\frac{t'}{d'}$ of $\frac{e}{N+1-2N^{\frac{1}{2}}}$, take $\varphi'(N) = \frac{ed'-1}{t'}$, $x' = \frac{N-\varphi'(N)+1}{2}$ and $y' = \sqrt{x'^2 - N}$. If $x', y' \in \mathbb{N}$, then the private key $(q, p, d) = (x' - y', x' + y', d')$.*

Therefore, the search of $\frac{t}{d}$ leading to solution (p, q, d) may be obtained from the class of convergent of $\frac{e}{N+1-2N^{\frac{1}{2}}}$. As convergent are approximations, the fraction $\frac{t}{d}$ is a rational approximation of $\frac{e}{N+1-2N^{\frac{1}{2}}}$. In the following theorem, we prove that (d, t) may be obtained as a short vector of quadratic form $q(x, y) = M\left(\bar{\alpha}x - y\right)^2 + \frac{1}{M}x^2$ for $\alpha = \frac{e}{N+1-2N^{\frac{1}{2}}}$.

Theorem 2.5. *Let $N = pq$, for $q < p < 2q$, be the modulus for RSA with $N^{\frac{1}{4}} \leq d < N^{\frac{3}{4}-\beta}$, $p - q = N^{\beta}$, $\beta \in (\frac{1}{4}, \frac{1}{2})$, e be the public enciphering exponent and d be the deciphering exponent, then for t such that $ed - 1 = \varphi(N)t$ and $\frac{t}{d}$, (d, t) is a short vector of a lattice $\mathbf{Z^2}$ equipped with a quadratic form*

$$q(x, y) = M\left(\frac{\bar{e}}{N+1-2N^{\frac{1}{2}}}x - y\right)^2 + \frac{1}{M}x^2$$

for an appropriate M.

Proof. First note for each choice of $M = 10^l$ for some l, and $\frac{\bar{e}}{N+1-2N^{\frac{1}{2}}}$ decimal approximation of $\frac{e}{N+1-2^{N^{\frac{1}{2}}}}$ to the precision $\frac{1}{M}$ we reduce the lattice $\mathbf{Z}^2$ with a quadratic form $q(x, y)$ in the variables x, y given as

$$q(x, y) = M\left(\frac{\bar{e}}{N+1-2N^{\frac{1}{2}}}x - y\right)^2 + \frac{1}{M}x^2$$

the 2-dimensional Gram-matrix for the above is given as

$$A = \begin{bmatrix} \left(\frac{\bar{e}}{N+1-2N^{\frac{1}{2}}}\right)^2 M + \frac{1}{M} & -\left(\frac{\bar{e}}{N+1-2N^{\frac{1}{2}}}\right)M \\ -\left(\frac{\bar{e}}{N+1-2N^{\frac{1}{2}}}\right)M & M \end{bmatrix}$$

.

and note the corresponding lattice in R^2 is given by the basis as columns of matrix B given as

$$B = \begin{bmatrix} \frac{1}{\sqrt{M}} & 0 \\ \left(\frac{\bar{e}}{N+1-2N^{\frac{1}{2}}}\right)\sqrt{M} & -\sqrt{M} \end{bmatrix}$$

which may be deduced by the results in *Lattices and Quadratic Forms* of [3]. Now applying LLL algorithm to B^T, we get reduced basis matrix B' and repeating the arguments as above we have a integer unimodular transformation matrix U

$$U = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

with (a,c) as short vector obtained for the choice of $M = 10^l$. Now note for any (v,u) such that $\frac{u}{v}$ is an approximation of $\frac{e}{N+1-2N^{\frac{1}{2}}}$, we have

$$\begin{aligned} q(v,u) &= M\left(\frac{\bar{e}}{N+1-2N^{\frac{1}{2}}}v-u\right)^2+\frac{1}{M}v^2 \\ &= Mv^2\left(\frac{\bar{e}}{N+1-2N^{\frac{1}{2}}}-\frac{u}{v}\right)^2+\frac{1}{M}v^2 \\ &= O\left(\frac{M}{v^2}\right)+O\left(\frac{v^2}{M}\right)+O(1) \end{aligned}$$

For any short vector (v,u) as $q(u,v) = O(1)$, note for $M \approx d^2$ the above holds for $v \ni v \approx d$. Therefore, by Theorem 2.3 as the required t,d are such that $\frac{t}{d}$ is an approximation to $\frac{e}{N+1-2N^{\frac{1}{2}}}$, (d,t) is a short vector for the given quadratic form $q(x,y) = M\left(\frac{\bar{e}}{N+1-2N^{\frac{1}{2}}}x-y\right)^2+\frac{1}{M}x^2$, for $M \approx d^2$. □

Note 1. *The search of convergent $\frac{t}{d}$ leading to solution (p,q,d) may be obtained from the class of short vectors (d,t) of*

$$q(x,y) = M\left(\frac{\bar{e}}{N+1-2N^{\frac{1}{2}}}x-y\right)^2+\frac{1}{M}x^2$$

for an appropriate choice of M.

In the following theorem, using lattice reduction we depicted the process of tracing the required (d,t) as short vector by varying M with respect to restrictions to d that are even beyond the Wiener Attack bound for d. This process can be interpreted as Wiener's extension with lattice reduction.

Theorem 2.6 (Wiener's extension in the range $N^{\frac{1}{4}} \leq d < N^{\frac{3}{4}-\beta}$ with Lattice Reduction)**.** *Let $N = pq$, $q < p < 2q$ be the modulus for RSA, e be the public enciphering exponent, d be the deciphering exponent for $N^{\frac{1}{4}} < d < N^{\frac{3}{4}-\beta}$ and $p-q = \Delta = N^\beta$, then there is a M such that (d,t) is a short vector of the quadratic form,*

$$q(x,y) = M\left(\frac{\bar{e}}{N+1-2N^{\frac{1}{2}}}x-y\right)^2+\frac{1}{M}x^2$$

where $\frac{\bar{e}}{N+1-2N^{\frac{1}{2}}}$ is a decimal approximation of $\frac{e}{N+1-2N^{\frac{1}{2}}}$ to precision $\frac{1}{M}$.

Proof. By Theorem 2.3 as the required t,d are such that $\frac{t}{d}$ is an approximation to $\frac{e}{N+1-2N^{\frac{1}{2}}}$, we have by above theorem that (d,t) is a short vector for a quadratic form

$$q(x,y) = M\left(\frac{\bar{e}}{N+1-2N^{\frac{1}{2}}}x-y\right)^2+\frac{1}{M}x^2$$

for $M = 10^l$ for some appropriate l, such that $d \approx \sqrt{M}$. The search for this M is described in the following: Let

$$r = \begin{cases} \frac{d(N)}{2} & \text{if } d(N) \text{ is even,} \\ \frac{d(N)+1}{2} & \text{if } d(N) \text{ is odd} \end{cases}$$

where $d(N)$ is the number of digits in N. Then for all s with $r \leq s < d(N)$, note $M_s = 10^s$ is such that $N^{\frac{1}{2}} < M_s < N$. Now note as d is such that $N^{\frac{1}{4}} < d < N^{\frac{3}{4}-\beta}$ for $\beta \in (\frac{1}{4},\frac{1}{2})$. Considering the maximum upper bound for d at $\beta = \frac{1}{4}$, we have $N^{\frac{1}{4}} < d < N^{\frac{1}{2}}$, this implies $N^{\frac{1}{2}} < d^2 < N$. Therefore, d^2 and M_s lie in the same range i.e., $N^{\frac{1}{2}} < M_s, d^2 < N$. Now varying s from r to $d(N)$, note as M_s gets close to d^2, $M_s \approx d^2$ i.e., $s \approx d(d^2)$ the short vector corresponding to such M_s gives the required (d,t). Note such M_s can be reached with utmost $\frac{d(N)}{2}$ variations for s. Further note for $d > N^{\frac{1}{2}}$, as d does not satisfy the hypothesis of theorem, note $\frac{t}{d}$ of the required (d,t) may not be a convergent of $\frac{e}{N+1-2N^{\frac{1}{2}}}$, hence it may not be an approximation and hence we cannot obtain (d,t) as a short vector of the quadratic form for some M for $d > N^{\frac{1}{2}}$. □

In the following theorem we describe the execution of the private key (p, q, d) using Wiener extension with Lattice Reduction:

Theorem 2.7. *Let $N^{\frac{1}{4}} \leq d < N^{\frac{3}{4}-\beta}$, $p - q = N^{\beta}$ and let $M = 10^s$ for $r \leq s \leq d(N)$, then for short vector (d_s, t_s) of the quadratic form,*

$$q(x, y) = M\left(\frac{\bar{e}}{N + 1 - 2N^{\frac{1}{2}}}x - y\right)^2 + \frac{1}{M}x^2$$

take $\varphi_s(N) = \frac{ed_s-1}{t_s}$, $x_s = \frac{N-\varphi_s(N)+1}{2}$ and $y_s = \sqrt{{x_s}^2 - N}$. If $x_s, y_s \in \mathbb{N}$, then (d_s, t_s) is the required short vector giving the private key $(q, p, d) = (x_s - y_s, x_s + y_s, d_s)$.

Proof. Suppose $x_s, y_s \in \mathbb{N}$ for some s in range $1 \leq s \leq r$, then by definition of y_s in theorem, we have

$$\begin{aligned} N &= x_s^2 - y_s^2 \\ &= (x_s + y_s)(x_s - y_s). \end{aligned}$$

Since $x_s + y_s, x_s - y_s \in \mathbb{N}$, they are the factors of N, i.e., $x_s + y_s, x_s - y_s$ are $1, p, q$ or N. Now as $p < q$ we have two cases:

(i). $x_s + y_s = N, x_s - y_s = 1,$

(ii). $x_s + y_s = p, x_s - y_s = q.$

Note Case (i) is not possible, for as $x_s + y_s = N$ and $x_s - y_s = 1$, then $\frac{N+1}{2} = x_s$,

$$\begin{aligned} \text{and} \qquad x_s &= \frac{N - \varphi_s(N) + 1}{2} \\ \Rightarrow \quad \frac{N+1}{2} &= \frac{N - \varphi_s(N) + 1}{2} \\ \Rightarrow \quad \frac{ed_s - 1}{t} &= 0 \\ \Rightarrow \qquad ed_s &= 1 \\ \Rightarrow \qquad e &= 1 \end{aligned}$$

which is not possible. Therefore, Case (i) is not possible since $e > 1$. Thus, the only possible Case is (ii). Therefore and we have $x_s + y_s = p$, $x_s - y_s = q$, whenever $x_s, y_s \in \mathbb{N}$. Now, we show that $d = d_s$. By definition of x_s we have

$$\begin{aligned} x_s &= \frac{N - \varphi_s(N) + 1}{2} \\ \Rightarrow \varphi_s(N) &= N - 2x_s + 1 \\ &= N - (q + p) + 1 \\ &= \varphi(N) \\ \Rightarrow d_s &\equiv d \mod \varphi(N) \end{aligned}$$

Now note that the short vector (d, t) is either (d_s, t_s) or obtained as a short vector in the later iterations for some $M = 10^l$, for $l > s$. Then as $M \approx d^2$, we have $d_s \leq d$. Therefore as $d < \varphi(N)$, we have $d_s \leq d < \varphi(N)$. Hence $d_s \equiv d \mod \varphi(N) \Rightarrow d = d_s$. □

An algorithm for the implementation of Wiener's extension in the range $N^{\frac{1}{4}} \leq d < N^{\frac{3}{4}-\beta}$ with lattice reduction is given in the following:

Algorithm:

Step 1: Start

Step 2: Input e, N.

Step 3: Compute $\frac{e}{N+1-2N^{\frac{1}{2}}}$ to $d(N)$ decimals, where

$$r = \begin{cases} \frac{d(N)}{2} & \text{if } \ d(N) \ \text{ is even,} \\ \frac{d(N)+1}{2} & \text{if } \ d(N) \ \text{ is odd.} \end{cases}$$

Step 4: Set $i = r$.

Step 5: Set $M = 10^i$, $\frac{\overline{e}}{N+1-2N^{\frac{1}{2}}} = \frac{e}{N+1-2N^{\frac{1}{2}}}$ corrected to i decimal places.

Step 6: Set

$$B = \begin{bmatrix} \frac{1}{\sqrt{M}} & 0 \\ \frac{\overline{e}}{N+1-2N^{\frac{1}{2}}} & -\sqrt{M} \end{bmatrix}$$

Apply LLL algorithm to B^T and then obtain unimodular transformation matrix $U = B^{-1}(B')^T$, where B' is the resultant obtained using LLL

$$U = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

Set $t_i = |c|, d_i = |a|$

Step 7: Compute $\varphi_i(N) = \frac{ed_i - 1}{t_i}$, $x_i = \frac{N - \varphi_i(N) + 1}{2}$, $y_i = \sqrt{x_i^2 - N}$.

Step 8: If $\varphi_i(N), x_i, y_i \in N$, then $(q, p, d) = (x_i - y_i, x_i + y_i, d_i)$, otherwise $i = i + 1$ and go to Step 5.

Example 2.8. Consider $(e, N) = (948120312068323160758410969049, 177471084031966797944323676863 3)$. Then the decimal representation of $\left(\frac{e}{N+1-2\sqrt{N}}\right)$ which is equal to $0.534239319740417757456566219402810274372359113 49\ldots$. Now, as N has 30 digits and is even, choose $M = 10^{\frac{d(N)}{2}} = 10^{15}$ and find the decimal expansion of $\left(\frac{e}{N+1-2\sqrt{N}}\right)$ corrected to 15 decimals. Thus, $\left(\frac{\overline{e}}{N+1-2\sqrt{N}}\right) = 0.534239319740418$. Now construct the matrix B and apply LLL algorithm to B^T :

$$B^T = \begin{bmatrix} 2524265620060144 6943299/79824287786472775821404714 1574 & 382736530102/22655 \\ 0 & -79824287786472775821404714 1574/2524265620060144 6943299 \end{bmatrix}$$

Now, the LLL matrix, B' is given by :

$$B' = \begin{bmatrix} 21987166364253519654205003227 8/39912143893236387910702357078 7 & -92624145646797102878218498/57187237622462578050043884 5 \\ 42039404878496716535720613878 7/79824287786472775821404714157 4 & 94954121155883733821394673 4/57187237622462578050043884 5 \end{bmatrix}$$

Finally, the unimodular integral transformation matrix is given by:

$$U = \begin{bmatrix} 17420644 & 16654113 \\ 9306793 & 8897282 \end{bmatrix}$$

Thus, the convergent obtained is $\frac{t}{d} = \left|\frac{9306793}{17420644}\right| = \frac{9306793}{17420644}$ and do not give integer values for $\varphi_s(N), x_s$ and y_s. Therefore, discarding this convergent, we update M to 10^{16} and consider 16 decimals of $\left(\frac{e}{N+1-2\sqrt{N}}\right)$. Thus, $\left(\frac{\overline{e}}{N+1-2\sqrt{N}}\right) =$

0.5342393197404178. Now proceeding as above, note we obtain the same convergent, so we again discard this convergent and next update M to 10^{17} and consider 17 decimals of the $\left(\frac{e}{N+1-2\sqrt{N}}\right)$. Thus, $\left(\frac{\bar{e}}{N+1-2\sqrt{N}}\right) = 0.53423931974041776$. Now construct the matrix B and apply LLL algorithm to B^T :

$$B^T = \begin{bmatrix} 27272480621782245960612/862431562076370278549170309642 1 & 4334864986046/25659 \\ \\ 0 & -79824287786472775821404714157 40/25242656200601446943299 \end{bmatrix}$$

Now, the LLL matrix, B' is given by :

$$B' = \begin{bmatrix} 2829719853610307547623124167796/8624315620763702785491703096421 & -2712382451640797644749129 38/6477013154512325271181090 41 \\ \\ -1367349509214257058571536116 4852/8624315620763702785491703096421 & -2211297531789016841143430 38/2159004384837441757060363 47 \end{bmatrix}$$

Finally, the unimodular integral transformation matrix is given by:

$$U = \begin{bmatrix} 103757333 & -501366021 \\ \\ 55431247 & -267849442 \end{bmatrix}$$

Now, required convergent is given by, $\frac{t}{d} = \mid \frac{-55431247}{103757333} \mid = \frac{55431247}{103757333}$ and we have

$$\begin{aligned} \varphi_s(N) &= \frac{ed-1}{t} = \frac{(9481203120683231607584109690 49)(103757333) - 1}{55431247} \\ &= 17747108403196652772834603462 28 \\ x_s &= \frac{N - \varphi_s(N) + 1}{2} = 1351079888211203 \\ y_s &= \sqrt{x_s^2 - N} = 225179981368524 \end{aligned}$$

Therefore as $\varphi_s(N), x_s$ and y_s are integers we have the private key given as

$$\begin{aligned} (q, p, d) &= (x_s - y_s, x_s + y_s, d) \\ &= (1125899906842679, 1576259869579727, 103757333). \end{aligned}$$

This process of varying M_s in the range $N^{\frac{1}{2}} < M_s < N$ and applying LLL to obtain $\frac{t_s}{d_s}$ leading to private key is depicted in the following table:

M	$\bar{\alpha} = \frac{\bar{e}}{N+1-2N^{\frac{1}{2}}}$	Unimodular matrix using LLL $U = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$	$\frac{t_s}{d_s} = \mid \frac{c}{a} \mid$	$\varphi_s(N) = \frac{ed_s-1}{t_s}$	$x_s = \frac{N-\varphi_s(N)+1}{2}$	$y_s = \sqrt{x_s{}^2 - N}$	$(q, p, d) = (x_s - y_s, x_s + y_s, d_s)$/Set M to iterate
$M = 10^{15}$	0.534239319740418	$U = \begin{bmatrix} 17420644 & 16654113 \\ 9306793 & 8897282 \end{bmatrix}$	$\frac{9306793}{17420644}$	$\notin \mathbb{N}$	$\notin \mathbb{N}$	$\notin \mathbb{N}$	Set $M = 10^{16}$
$M = 10^{16}$	0.5342393197404178	$U = \begin{bmatrix} 17420644 & 103757333 \\ 9306793 & 55431247 \end{bmatrix}$	$\frac{9306793}{17420644}$	$\notin \mathbb{N}$	$\notin \mathbb{N}$	$\notin \mathbb{N}$	Set $M = 10^{17}$
$M = 10^{17}$	0.53423931974041776	$U = \begin{bmatrix} 103757333 & -501366021 \\ 55431247 & -267849442 \end{bmatrix}$	$\frac{55431247}{103757333}$	17747108403196652772834603-46228	1351079888211203	225179981368524	(1125899906842679, 1576259869579727, 103757333)

Table 1: Implementation of Wiener's extension in the range $N^{\frac{1}{4}} \leq d < N^{\frac{3}{4}-\beta}$ with Lattice Reduction.

3. Implementing Wiener's Extension in the Range $N^{\frac{1}{4}} \leq d < N^{(\frac{1-\gamma}{2})}$, $\gamma \leq \frac{1}{2}$ with Lattice Reduction

For $q < p < 2q$, the maximum difference between p and q is $\sqrt{N}$. In this section, if $|\rho q - p| \leq \frac{N^\gamma}{16}$ for $1 \leq \rho \leq 2$, $\gamma \leq \frac{1}{2}$, then the RSA is insecure when $d = N^\delta$ and $\delta < \frac{1}{2} - \frac{\gamma}{2}$.

Lemma 3.1. *Let $|p - \rho q| \leq \frac{N^\gamma}{16}$, where $\gamma \leq \frac{1}{2}$ and $1 \leq \rho \leq 2$. Then*

$$\left| p + q - \left(\sqrt{\rho} + \frac{1}{\sqrt{\rho}} \right) \sqrt{N} \right| < \frac{N^\gamma}{8}.$$

Theorem 3.2. *Let $|p - \rho q| \leq \frac{N^\gamma}{16}$ with $1 \leq \rho \leq 2$, $\gamma \leq \frac{1}{2}$ and $d = N^\delta$ and $\delta < \frac{1}{2} - \frac{\gamma}{2}$ then*

$$\left| \frac{e}{N - \left(\sqrt{\rho} + \frac{1}{\sqrt{\rho}} \right) \sqrt{N} + 1} - \frac{t}{d} \right| \leq \frac{1}{2d^2}$$

Hence by approximation theorem it follows that $\frac{t}{d}$ is a convergent of $\frac{e}{N - \left(\sqrt{\rho} + \frac{1}{\sqrt{\rho}}\right)\sqrt{N} + 1}$. Thus, $\frac{t}{d}$ is obtained from the list of convergent of $\frac{e}{N - \left(\sqrt{\rho} + \frac{1}{\sqrt{\rho}}\right)\sqrt{N} + 1}$ using continued fractions. This Wiener's extension attack on RSA basically searches the convergent $\frac{t}{d}$ from the class of convergent of $\frac{e}{N - \left(\sqrt{\rho} + \frac{1}{\sqrt{\rho}}\right)\sqrt{N} + 1}$ that lead to (p, q, d) whenever $\delta < \frac{1}{2} - \frac{\gamma}{2}$.

Theorem 3.3 (Wiener's extension in the range $N^{\frac{1}{4}} \leq d < N^{(\frac{1-\gamma}{2})}$, $\gamma \leq \frac{1}{2}$). *Let $N^{\frac{1}{4}} \leq d < N^{(\frac{1-\gamma}{2})}$, $\gamma \leq \frac{1}{2}$ and for any convergent $\frac{t'}{d'}$ of, $\frac{e}{N - \left(\sqrt{\rho} + \frac{1}{\sqrt{\rho}}\right)\sqrt{N} + 1}$ take $\varphi'(N) = \frac{ed'-1}{t'}$, $x' = \frac{N - \varphi'(N) + 1}{2}$ and $y' = \sqrt{x'^2 - N}$. If $x', y' \in \mathbb{N}$, then the private key $(q, p, d) = (x' - y', x' + y', d')$.*

Therefore, the search of $\frac{t}{d}$ leading to solution (p, q, d) may be obtained from the class of convergent of $\frac{e}{N - \left(\sqrt{\rho} + \frac{1}{\sqrt{\rho}}\right)\sqrt{N} + 1}$. As convergent are approximations, the fraction $\frac{t}{d}$ is a rational approximation of $\frac{e}{N - \left(\sqrt{\rho} + \frac{1}{\sqrt{\rho}}\right)\sqrt{N} + 1}$. In the following theorem, we prove that (d, t) may be obtained as a short vector of quadratic form $q(x, y) = M \left(\bar{\alpha}x - y\right)^2 + \frac{1}{M}x^2$ for $\alpha = \frac{e}{N - \left(\sqrt{\rho} + \frac{1}{\sqrt{\rho}}\right)\sqrt{N} + 1}$.

Theorem 3.4. *Let $N = pq$, for $q < p < 2q$ be the modulus for RSA and $N^{\frac{1}{4}} \leq d < N^{(\frac{1-\gamma}{2})}, \gamma \leq \frac{1}{2}$, e be the public enciphering exponent and d be the deciphering exponent. Then for t such that $ed - 1 = \varphi(N)t$, (d, t) is a short vector of a lattice $\mathbf{Z^2}$ equipped with a quadratic form*

$$q(x, y) = M \left(\frac{\bar{e}}{N - \left(\sqrt{\rho} + \frac{1}{\sqrt{\rho}} \right) \sqrt{N} + 1} x - y \right)^2 + \frac{1}{M} x^2$$

for an appropriate M.

Proof. First note for each choice of $M = 10^l$ for some l, $\frac{\bar{e}}{N - \left(\sqrt{\rho} + \frac{1}{\sqrt{\rho}}\right)\sqrt{N} + 1}$ and decimal approximation of $\frac{e}{N - \left(\sqrt{\rho} + \frac{1}{\sqrt{\rho}}\right)\sqrt{N} + 1}$ to the precision $\frac{1}{M}$ we reduce the lattice $\mathbf{Z}^2$ with a quadratic form $q(x, y)$ in the variables x, y given as and

$$q(x, y) = M \left(\frac{\bar{e}}{N - \left(\sqrt{\rho} + \frac{1}{\sqrt{\rho}} \right) \sqrt{N} + 1} x - y \right)^2 + \frac{1}{M} x^2$$

the 2-dimensional Gram-matrix for the above is given as

$$A = \begin{bmatrix} \left(\frac{\bar{e}}{N - \left(\sqrt{\rho} + \frac{1}{\sqrt{\rho}}\right)\sqrt{N} + 1} \right)^2 M + \frac{1}{M} & -\left(\frac{\bar{e}}{N - \left(\sqrt{\rho} + \frac{1}{\sqrt{\rho}}\right)\sqrt{N} + 1} \right) M \\ & \\ -\left(\frac{\bar{e}}{N - \left(\sqrt{\rho} + \frac{1}{\sqrt{\rho}}\right)\sqrt{N} + 1} \right) M & M \end{bmatrix}$$

and note the corresponding lattice in R^2 is given by the basis as columns of matrix B given as

$$B = \begin{bmatrix} \frac{1}{\sqrt{M}} & 0 \\ \left(\frac{\bar{e}}{N-\left(\sqrt{\rho}+\frac{1}{\sqrt{\rho}}\right)\sqrt{N}+1}\right)\sqrt{M} & -\sqrt{M} \end{bmatrix}$$

which may be deduced by the results in *Lattices and Quadratic Forms* of [4]. Now applying LLL algorithm to B^T, we get reduced basis matrix B' and repeating the arguments as above we have a integer unimodular transformation matrix U

$$U = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

with (a, c) as short vector obtained for the choice of $M = 10^l$. Now note for any (v, u) such that $\frac{u}{v}$ is an approximation of $\frac{e}{N}$, we have

$$\begin{aligned} q(v,u) &= M\left(\frac{\bar{e}}{N-\left(\sqrt{\rho}+\frac{1}{\sqrt{\rho}}\right)\sqrt{N}+1}v-u\right)^2+\frac{1}{M}v^2 \\ &= Mv^2\left(\frac{\bar{e}}{N-\left(\sqrt{\rho}+\frac{1}{\sqrt{\rho}}\right)\sqrt{N}+1}-\frac{u}{v}\right)^2+\frac{1}{M}v^2 \\ &= O(\frac{M}{v^2})+O(\frac{v^2}{M})+O(1) \end{aligned}$$

For any short vector (v, u) as $q(u, v) = O(1)$, note for $M \approx d^2$ the above holds for $v \ni v \approx d$. Therefore by Theorem 3.2 as the required t, d are such that $\frac{t}{d}$ is an approximation to $\frac{e}{N-\left(\sqrt{\rho}+\frac{1}{\sqrt{\rho}}\right)\sqrt{N}+1}$ and (d, t) is a short vector for the given quadratic form $q(x,y) = M\left(\frac{\bar{e}}{N-\left(\sqrt{\rho}+\frac{1}{\sqrt{\rho}}\right)\sqrt{N}+1}x-y\right)^2+\frac{1}{M}x^2$, for $M \approx d^2$. □

Note 2. *The search of convergent $\frac{t}{d}$ leading to solution (p, q, d) may be obtained from the class of short vectors*

$$q(x,y) = M\left(\frac{\bar{e}}{N-\left(\sqrt{\rho}+\frac{1}{\sqrt{\rho}}\right)\sqrt{N}+1}x-y\right)^2+\frac{1}{M}x^2$$

for an appropriate choice of M.

In the following theorem, using lattice reduction we depicted the process of tracing the required (d, t) as short vector by varying M with respect to restrictions to d that are even beyond the Wiener Attack bound for d. This process can be interpreted as Wiener Attack extension via lattice reduction.

Theorem 3.5 (Wiener's Extension in the Range $N^{\frac{1}{4}} \leq d < N^{(\frac{1-\gamma}{2})}, \gamma \leq \frac{1}{2}$ with Lattice Reduction)**.** *Let $N = pq$, $q < p < 2q$ be the modulus for RSA, e be the public enciphering exponent, d be the deciphering exponent such that $N^{\frac{1}{4}} \leq d < N^{(\frac{1-\gamma}{2})}, \gamma \leq \frac{1}{2}$, $|p - \rho q| \leq \frac{N^\gamma}{16}$, $1 \leq \rho \leq 2$,, then there is a M such that (d, t) is a short vector of a quadratic form,*

$$q(x,y) = M\left(\frac{\bar{e}}{N-\left(\sqrt{\rho}+\frac{1}{\sqrt{\rho}}\right)\sqrt{N}+1}x-y\right)^2+\frac{1}{M}x^2$$

$\frac{\bar{e}}{N-\left(\sqrt{\rho}+\frac{1}{\sqrt{\rho}}\right)\sqrt{N}+1}$ *is a decimal approximation of* $\frac{e}{N-\left(\sqrt{\rho}+\frac{1}{\sqrt{\rho}}\right)\sqrt{N}+1}$ *to precision* $\frac{1}{M}$.

Proof. By Theorem 3.2 as the required t, d are such that $\frac{t}{d}$ is an approximation to $\frac{e}{N-\left(\sqrt{\rho}+\frac{1}{\sqrt{\rho}}\right)\sqrt{N}+1}$, we have by above theorem that (d,t) is a short vector for a quadratic form

$$q(x,y) = M\left(\frac{\bar{e}}{N-\left(\sqrt{\rho}+\frac{1}{\sqrt{\rho}}\right)\sqrt{N}+1}x - y\right)^2 + \frac{1}{M}x^2$$

for $M = 10^l$ for some appropriate l, such that $d \approx \sqrt{M}$. The search for this M is described below:

Let

$$r = \begin{cases} \frac{d(N)}{2} & \text{if } \ d(N) \ \text{ is even,} \\ \frac{d(N)+1}{2} & \text{if } \ d(N) \ \text{ is odd} \end{cases}$$

where $d(N)$ is the number of digits in N. Then for all s with $r \leq s < d(N)$, note $M_s = 10^s$ is such that $N^{\frac{1}{2}} < M_s < N$. Now note as d is such that $N^{\frac{1}{4}} \leq d < N^{(\frac{1-\gamma}{2})}$, $|\rho q - p| \leq \frac{N^\gamma}{16}$, $1 \leq \rho \leq 2$, $\gamma \leq \frac{1}{2}$, considering the maximum upper bound for d at $\gamma \approx 0$, we have $N^{\frac{1}{4}} < d < N^{\frac{1}{2}}$, this implies $N^{\frac{1}{2}} < d^2 < N$. Therefore, d^2 and M_s lie in the same range i.e., $N^{\frac{1}{2}} < M_s, d^2 < N$. Now varying s from r to $d(N)$, note as M_s gets close to d^2, $M_s \approx d^2$ i.e., $s \approx d(d^2)$, the short vector corresponding to such M_s gives the required (d,t). Note such M_s can be reached with utmost $\frac{d(N)}{2}$ variations for s. Further note for $d > N^{\frac{1}{2}}$, as d does not satisfy the hypothesis of theorem, note $\frac{t}{d}$ of the required (d,t) may not be a convergent of $\frac{e}{N-\left(\sqrt{\rho}+\frac{1}{\sqrt{\rho}}\right)\sqrt{N}+1}$, hence it may not be an approximation and hence we cannot obtain (d,t) as a short vector of the quadratic form for some M for $d > N^{\frac{1}{2}}$. □

In the following theorem we describe the execution of the private key (p,q,d) using Wiener extension with Lattice Reduction:

Theorem 3.6. *Let $|p - \rho q| \leq \frac{N^\gamma}{16}$ with $1 \leq \rho \leq 2$, $\gamma \leq \frac{1}{2}$, $d = N^\delta$ and $\delta < \frac{1}{2} - \frac{\gamma}{2}$ and let $M = 10^s$ for $r \leq s \leq d(N)$, then for short vector (d_s, t_s) of the quadratic form,*

$$q(x,y) = M\left(\frac{\bar{e}}{N-\left(\sqrt{\rho}+\frac{1}{\sqrt{\rho}}\right)\sqrt{N}+1}x - y\right)^2 + \frac{1}{M}x^2$$

take $\varphi_s(N) = \frac{ed_s-1}{t_s}$, $x_s = \frac{N-\varphi_s(N)+1}{2}$ and $y_s = \sqrt{{x_s}^2 - N}$. If $x_s, y_s \in \mathbb{N}$, then (d_s, t_s) is the required short vector giving the private key $(q,p,d) = (x_s - y_s, x_s + y_s, d_s)$.

Proof. The proof is same as the proof of Theorem 3.5. □

An algorithm for the implementation of Wiener's extension in the range $N^{\frac{1}{4}} \leq d < N^{(\frac{1-\gamma}{2})}, \gamma \leq \frac{1}{2}$ with lattice reduction is given in the following:

Algorithm:

Step 1: Start

Step 2: Input e, N.

Step 3: Compute $\frac{e}{N-\left(\sqrt{\rho}+\frac{1}{\sqrt{\rho}}\right)\sqrt{N}+1}$ to $d(N)$ decimals, where

$$r = \begin{cases} \frac{d(N)}{2} & \text{if } \ d(N) \ \text{ is even,} \\ \frac{d(N)+1}{2} & \text{if } \ d(N) \ \text{ is odd.} \end{cases}$$

Step 4: Set $i = r$.

Step 5: Set $M = 10^i$, $\frac{\bar{e}}{N-\left(\sqrt{\rho}+\frac{1}{\sqrt{\rho}}\right)\sqrt{N}+1} = \frac{e}{N-\left(\sqrt{\rho}+\frac{1}{\sqrt{\rho}}\right)\sqrt{N}+1}$ corrected to i decimal places.

Step 6: Set

$$B = \begin{bmatrix} \frac{1}{\sqrt{M}} & 0 \\ \frac{\bar{e}}{N-\left(\sqrt{\rho}+\frac{1}{\sqrt{\rho}}\right)\sqrt{N}+1}\sqrt{M} & -\sqrt{M} \end{bmatrix}$$

Apply LLL algorithm to B^T and then obtain unimodular transformation matrix $U = B^{-1}(B')^T$, where B' is the resultant obtained using LLL

$$U = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

Set $t_i = |c|, d_i = |a|$

Step 7: Compute $\varphi_i(N) = \frac{ed_i-1}{t_i}$, $x_i = \frac{N-\varphi_i(N)+1}{2}$, $y_i = \sqrt{x_i^2 - N}$.

Step 8: If $\varphi_i(N)$, $x_i, y_i \in N$, then $(q,p,d) = (x_i - y_i, x_i + y_i, d_i)$, otherwise $i = i+1$ and go to Step 5.

Example 3.7. *Consider* $(e,N) = (1242349, 2035153)$. *Then the decimal representation of* $\left(\frac{e}{N-\left(\sqrt{\rho}+\frac{1}{\sqrt{\rho}}\right)\sqrt{N}+1}\right)$ *which is equal to* $0.611353789122353\ldots$. *Now, as* N *has 7 digits and is odd, choose* $M = 10^{\frac{d(N)+1}{2}} = 10^4$ *and find the decimal expansion of* $\left(\frac{e}{N-\left(\sqrt{\rho}+\frac{1}{\sqrt{\rho}}\right)\sqrt{N}+1}\right)$ *corrected to 4 decimals. Thus,* $\frac{\bar{e}}{N-\left(\sqrt{\rho}+\frac{1}{\sqrt{\rho}}\right)\sqrt{N}+1} = \frac{e}{N-\left(\sqrt{\rho}+\frac{1}{\sqrt{\rho}}\right)\sqrt{N}+1} = 0.6114$. *Choosing* $M = 10^4$, *we didn't get the desired convergent. Hence update* M *as* $M = 10^5$ *and find the next convergent by considering 5 decimals of* $\left(\frac{\bar{e}}{N-\left(\sqrt{\rho}+\frac{1}{\sqrt{\rho}}\right)\sqrt{N}+1}\right)$, $\bar{\alpha} = 0.61135$. *Now construct the matrix* B *and apply LLL algorithm to* B^T *:*

$$B^T = \begin{bmatrix} 9815920/3104066453 & 1633031337/8447041 \\ 0 & -2709261463/8567437 \end{bmatrix}$$

Now, the LLL matrix, B' *is given by :*

$$B' = \begin{bmatrix} 2247845680/3104066453 & -19452456259019/72369491603917 \\ -2424532240/3104066453 & -78954087169010/72369491603917 \end{bmatrix}$$

Finally, the unimodular integral transformation matrix is given by:

$$U = \begin{bmatrix} 229 & -247 \\ 140 & -151 \end{bmatrix}$$

Now, required convergent is given by, $\frac{t}{d} = \left|\frac{140}{229}\right| = \frac{140}{229}$ *and we have:*

$$\begin{aligned} \varphi_s(N) &= \frac{ed-1}{t} \\ &= \frac{(1242349)(229)-1}{140} \\ &= 2032128, \\ x_s &= \frac{N-\varphi_s(N)+1}{2} = 1513 \\ y_s &= \sqrt{x_s^2 - N} = 504. \end{aligned}$$

Therefore as $\varphi_s(N), x_s$ *and* y_s *are integers we have the private key given as* $(q,p,d) = (x_s - y_s, x_s + y_s, d) = (1009, 2017, 229)$.

This process of varying M_s in the range $N^{\frac{1}{2}} < M_s < N$ and applying LLL to obtain $\frac{t_s}{d_s}$ leading to private key is depicted in the following table:

M	$\left(\frac{\bar{e}}{N-\left(\sqrt{\rho}+\frac{1}{\sqrt{\rho}}\right)\sqrt{N}+1}\right)$	Unimodular matrix using LLL U	$\frac{t_s}{d_s} = \mid \frac{c}{a} \mid$	$\varphi_s(N) = \frac{ed_s-1}{t_s}$	$x_s = \frac{N-\varphi_s(N)+1}{2}$	$y_s = \sqrt{x_s{}^2 - N}$	$(q,p,d) = (x_s - y_s, x_s + y_s, d_s)$/ Set M to iterate
$M = 10^4$	0.6114	$U = \begin{bmatrix} -18 & 175 \\ -11 & 107 \end{bmatrix}$	$\frac{11}{18}$	$\notin \mathbb{N}$	$\notin \mathbb{N}$	$\notin \mathbb{N}$	Set $M = 10^5$
$M = 10^5$	0.61135	$U = \begin{bmatrix} 229 & -247 \\ 140 & -151 \end{bmatrix}$	$\frac{140}{229}$	2032128	1513	504	(1009, 2017,229)

Table 2: Implementation of Wiener's extension in the range $N^{\frac{1}{4}} \leq d < N^{(\frac{1-\gamma}{2})}, \gamma \leq \frac{1}{2}$ with Lattice Reduction.

4. Conclusion

The main idea of Wiener Attack that whenever $d < \frac{N^{1/4}}{\sqrt{6}}$, the fraction $\frac{t}{d}$ is a convergent of $\frac{e}{N}$ and hence it is interpreted as finding (d,t) as a short vector by reducing the quadratic form $q(x,y) = M\left(\frac{\bar{e}}{N}x - y\right)^2 + \frac{1}{M}x^2$ for an appropriate choice of M in our paper [8]. In this paper, we adapt these ideas to Wiener Attack extensions in the range $N^{\frac{1}{4}} \leq d < N^{\frac{3}{4}-\beta}$, $p - q = N^{\beta}$ and $N^{\frac{1}{4}} \leq d < N^{(\frac{1-\gamma}{2})}$, $\gamma \leq \frac{1}{2}$ with lattice reduction. The continued fraction based arguments of Wiener Attack extensions are implemented with the lattice based arguments and the LLL algorithm is used for reducing a basis of a lattice. This method is implemented as LLL comes close to solve SVP in smaller dimensions.

References

[1] Tom M. Apostol, *Introduction to Analytical Number Theory*, Springer International student edition, Narosa Publishing House.

[2] David M. Burton, *Elementary Number Theory*, Second Edition, Universal Book Stall, New Delhi, (2002).

[3] H. Cohen, *A course in Computational Algebraic Number Theory*, Graduate Texts in Math. 138. Springer, (1996).

[4] S. C. Coutinho, *The Mathematics of Ciphers*, University Press.

[5] H. Davenport, *The Higher Arithmetic*, Cambridge University Press, Eighth edition, (2008).

[6] Jeffery Hoftstein, Jill Pipher and Joseph H. Silverman, *An Introduction to Mathematical Cryptography*, Springer, (2008).

[7] P. Anuradha Kameswari and L. Jyotsna, *Extending Wiener's Extension to RSA-Like Cryptosystems over Elliptic Curves*, British Journal of Mathematics and Computer Science, 14(1)(2016), 1-8.

[8] P. Anuradha Kameswari and S. B. T. Sundari Katakam, *Implementing Wiener Attack with Lattice Reduction*, Journal of Global Research in Mathematical Archives, 6(1)(2019), 7-14.

[9] Neal Koblitz, *A course in Number Theory and cryptography*, Graduate Texts in Mathematics, Second edition, Springer.

[10] A. K. Lenstra, H. W. Lenstra and L. Lovasz, *Factoring Polynomials with Rational coefficients*, Math. Ann., 261(1982), 515-534.

[11] Phong Q. Nguyen and Brigitte Vallee, *The LLL Algorithm, Survey and Applications*, Springer, (2010).

[12] Nigel P. Smart, *The Algorithmic Resolution of Diophantine Equations*, London Mathematical Society, (1998).

[13] Michael J. Wiener, *Cryptanalysis of short RSA secret exponent*, IEEE. Transaction on Information Theory, 36(3)(1990), 553-558.